










COMP90082-2024-lp-koala	2
Product	3
Project Introduction	4
Production Demonstration Guide	6
Requirements	8
Persona	9
Prototype	10
Motivational Model	12
User Stories	13
Non-Functional Requirements	16
Sprint	17
Sprint 1	18
Plan For Sprint 2 and Sprint 3	19
Sprint 1 Review	21
Sprint 2	22
Plan For Sprint 3	23
Sprint 3	24
Ethics and Security	25
Cyber Security	26
Ethical Considerations	31
Meetings	32
Client Meetings	33
14/03/2024 Client Meeting	34
07/03/2024 Client Meeting	36
11/04/2024 Client Meeting	37
Mentor Meetings	38
06/03/2024 Mentor Meeting	39
12/03/2024 Mentor Meeting	40
19/03/2024 Mentor Meeting	41
16/04/2024 Mentor Meeting	42
23/04/2024 Mentor meeting	43
30/04/2024 Mentor meeting	44
Team Meetings	45
13/03/2024 Team Meeting	46
11/03/2024 Team Meeting	47
09/03/2024 Team Meeting	48
21/04/2024 Team Meeting	49
AI Code Review	50
Sprint 2 Code Review	51

Process Documentation

 Sprint Plannings	 Meetings	 Code Reviews
 Ethics and Security		

Product Documentation

 Product Guide	 Prototypes	 User stoires
 Persona	 Motivational Models	

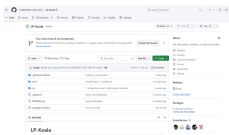
Quick Links



Deployed Product



Trello Board



Github

Product

[Project Introduction](#)

[Production Demonstration Guide](#)

Project Introduction

Project Overview

The DLASSP project is conceived as a comprehensive and customisable LMS, tailored specifically for a unique user system consisting of Admins, Researchers, and Raters. The platform is intended to provide a versatile digital environment where the users can manage, participate in, and evaluate a variety of educational and assessment-oriented projects. Each user group is granted access privileges aligned with their operational scope and responsibilities to facilitate efficient project management, content creation, user interaction, and data analysis.

Current Background

The recent increase in demand for digital platforms that support detailed project management and evaluation, particularly in education, underscores the need for an advanced LMS. Traditional LMSs often lack the specialised tools required to meet the intricate requirements of researchers and raters. Consequently, there exists a significant market gap for a more sophisticated product that can effectively address these needs. As educational institutions and organisations increasingly rely on digital platforms for teaching, learning, and assessment, the necessity for an enhanced LMS that offers comprehensive project management and evaluation capabilities becomes even more apparent.

Thus, the necessity for DLASSP arises from these critical gaps. As educational institutions and organisations increasingly rely on digital platforms for a broader range of functions—including in-depth project management, personalised learning experiences, and comprehensive evaluation mechanisms—the need for an enhanced LMS that integrates these advanced features becomes paramount. DLASSP is envisioned as a solution that not only supports the traditional roles of an LMS but also equips Admins, Researchers, and Raters with sophisticated tools specifically designed to address their unique challenges in managing, participating in, and evaluating educational and assessment-oriented projects. Through DLASSP, users will gain the ability to manage and evaluate educational content and projects with greater precision and flexibility, leading to improved educational outcomes and more effective research and assessment methodologies.

Project Goals

- **Develop a Customisable and Secure LMS:** Create a platform that can be tailored to the roles of Admin, Researchers, and Raters, ensuring secure and correct access to content and features according to user roles.
- **Enable Efficient Project and User Management:** Implement comprehensive administrative functions for user management.
- **Facilitate Specialised Content Creation and Management:** Equip researchers with advanced tools for creating, editing, and managing educational content.
- **Enhance Rater Interaction and Engagement:** Allow raters to engage with the content through interactive activities and provide meaningful feedback.
- **Ensure Data Security and Integrity:** Prioritise the protection of sensitive information.
- **Establish a Collaborative Environment:** Build forums where users can share insights, discuss evaluations, and contribute to the collective knowledge base.

Out Of Scope

- Enable admin/researchers to communicate with selected raters only in the forums
- Enable researchers to lock raters' ratings for a while

Trello Link

 [COMP90082](#)

Github Link

 <https://github.com/COMP90082-2024-SM1/LP-Koala> Connect your Github account

Our Team

Name	Role	Email
Weiyang Wu	Product Owner	weiyang1@student.unimelb.edu.au
Haofeng Chen	Scrum Master	haofengc@student.unimelb.edu.au
Gaoyuan Ou	Front-end Developer	gaoyuano@student.unimelb.edu.au
Mingxin Li	UX/UI Designer	mingxinl2@student.unimelb.edu.au
Yujin Du	Back-end Developer	yujind1@student.unimelb.edu.au
Qinglin Zhao	Back-end Developer	qinglinz@student.unimelb.edu.au

Stakeholders

Name	Role	Email
Sally O'Hagan	Client	sohagan@unimelb.edu.au
Ivy Chen	Client assistant	ivy.chen@unimelb.edu.au
Lin Li	Supervisor	lin.li10@unimelb.edu.au

Production Demonstration Guide

Usage

Link:

Please click the following link to access our product to check our progress:

- [LP-Koala project](#)

Test accounts:

There are three accounts for testing currently:

1. username: admin

password: password

2. username: researcher

password: password

3. username: rater1

password: password

Side notes:

Feel free to create user accounts using the admin account. For security reasons, we design the user creation only available via admin's portal, instead of users creating an account and waiting for admin's approval.

Functionalities are implemented according to project requirements. There is no need for instruction as our UI design is user-friendly and intuitive.

Since this is our temporary version of our project, some functionalities are not yet implemented. Some functionalities are subject to change for completeness and robustness. Further updates will be available in the later weeks.

Configuration

Login token expiry time:

Currently, once a user logs in, the login token will be expired in 5 minutes and the user will have to login again. We set this time to demonstrate the JWT expiry functionality. This is subject to change later according to client's needs.

Website domain name:

Since we deploy our project via Heroku for demonstration purposes for now, the domain name is <https://lp-koala-frontend-1e10ff20d284.herokuapp.com/>. This is subject to change later in the subject.

Deployment method

Our project is currently deployed using Heroku, as discussed in the plan for sprint 2. This project will be further deployed in the server provided by client when the product is ready for production.

Requirements

Persona

Prototype

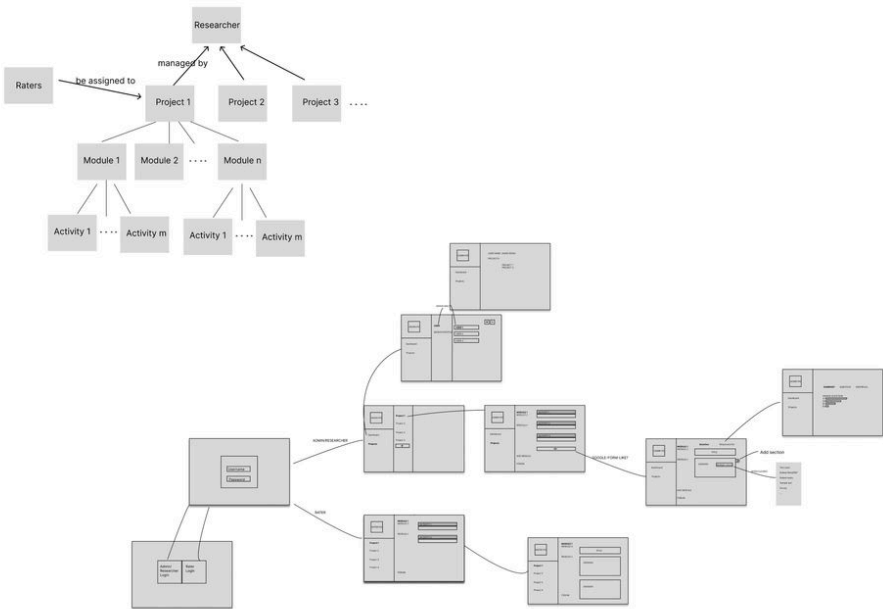
Motivational Model

User Stories

Prototype

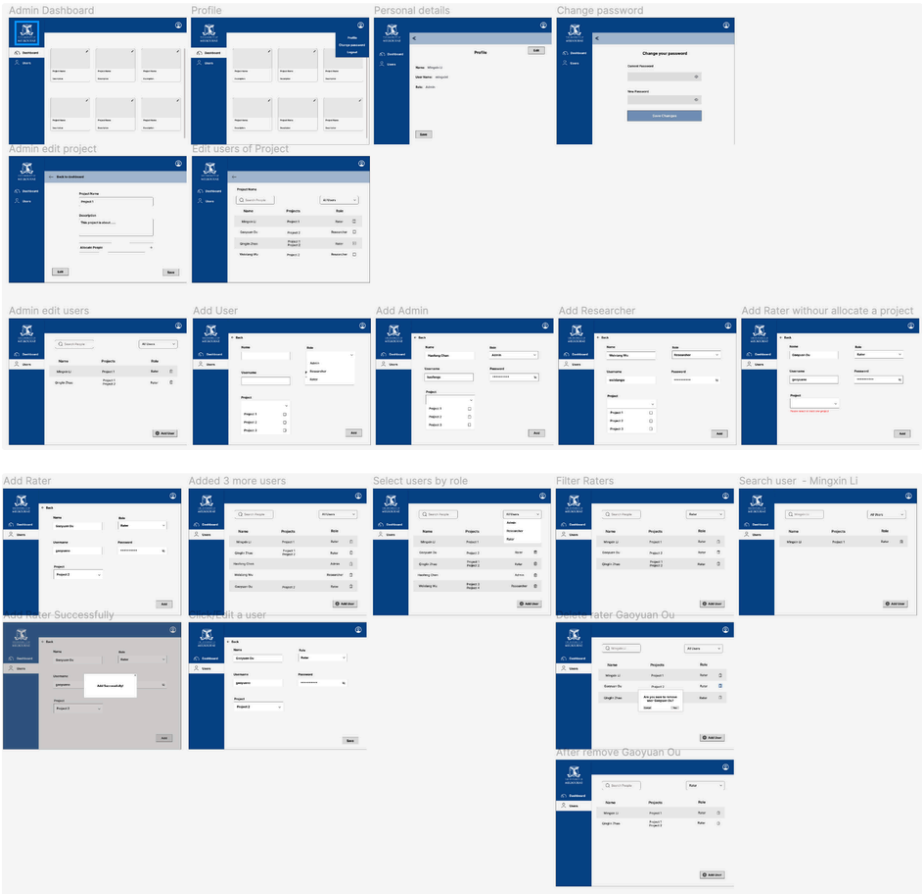
Low Fidelity Prototype

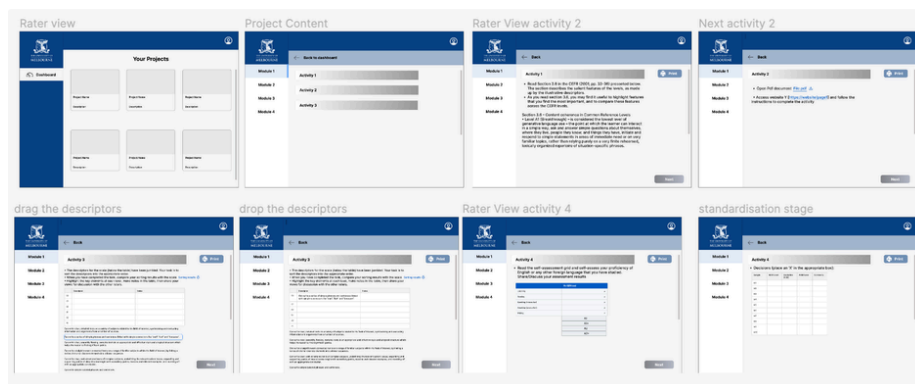
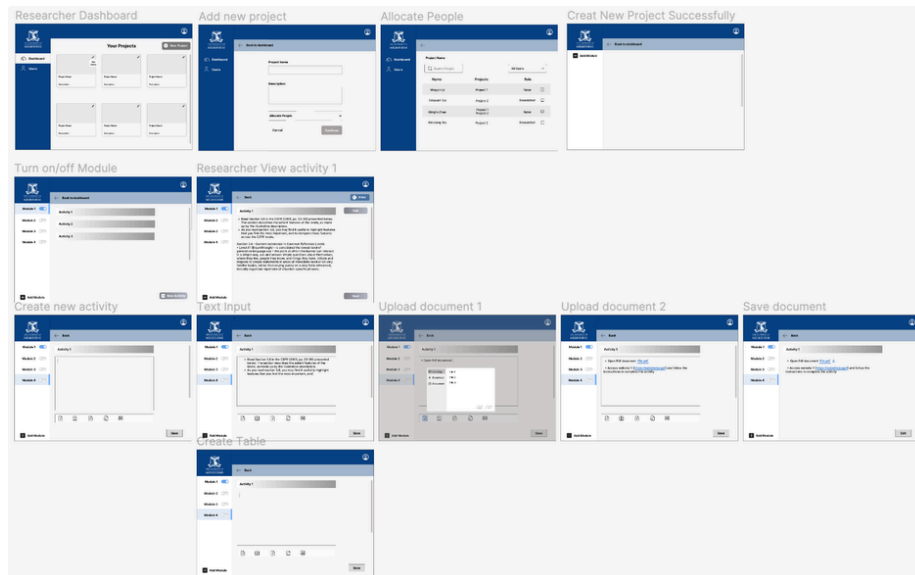
[Figma Link](#)



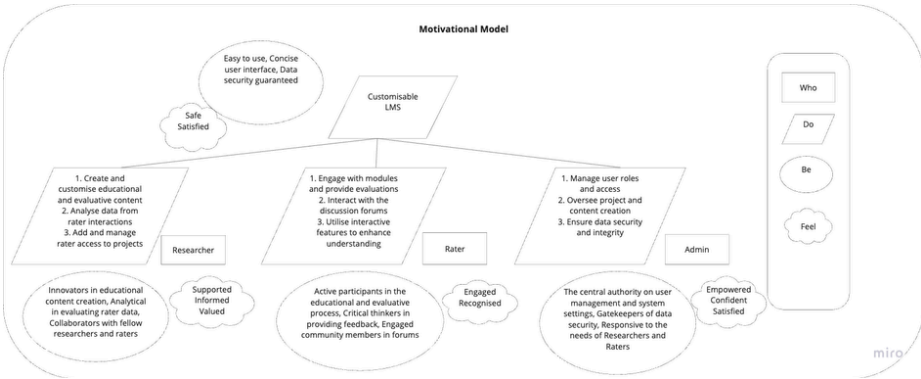
High Fidelity Prototype

[Figma link](#)





Motivational Model



Do/Be/Feel

Role	Do(Functional Goal)	Be(Quality Goal)	Feel(Emotional Goal)
Admin	<ul style="list-style-type: none">• Manage user roles and access• Oversee project and content creation• Ensure data security and integrity	<ul style="list-style-type: none">• The central authority on user management and system settings• Gatekeepers of data security• Responsive to the needs of Researchers and Raters	<ul style="list-style-type: none">• Empowered to maintain a robust and secure system• Confident in managing a user-friendly platform• Satisfied with the system's performance and reliability
Researcher	<ul style="list-style-type: none">• Create and customise educational and evaluative content• Analyse data from rater interactions• Add and manage rater access to projects	<ul style="list-style-type: none">• Innovators in educational content creation• Analytical in evaluating rater data• Collaborators with fellow researchers and raters	<ul style="list-style-type: none">• Supported by tools that facilitate creative content development• Informed by comprehensive data analytics• Valued for their contributions to the project's success
Rater	<ul style="list-style-type: none">• Engage with modules and provide evaluations• Interact with the discussion forums• Utilise interactive features to enhance understanding	<ul style="list-style-type: none">• Active participants in the educational and evaluative process• Critical thinkers in providing feedback• Engaged community members in forums	<ul style="list-style-type: none">• Engaged by interactive and relevant content• Recognised for their input and evaluations• Part of a larger community of practice

Do/Be/Feel List

User Stories

We use story points from 1 to 5 to estimate the complexity, effort, and time required to complete a task or feature, where each number represents an increasing level of complexity and effort needed. Story point 1 means it is trivial to complete a task while story point 5 demonstrates extremely difficult to finish a task.

Epic 1 - User Management

No.	As a <Role>	I want to <Do something>	So that <achieve some goals>	Priority	Task Size
1	Users (Admin/Researcher/Rater)	Log into account	I can access account information/ change profile etc..	High	2
2	Users (Admin/Researcher/Rater)	Update passwords	I can keep my data and my account safe	High	1
3	Users (Admin/Researcher/Rater)	Edit names	A new name can be displayed on discussion forums and all the old posts	Medium	1
4	Admin	Add or remove users with assigned roles	I can create admins for administration. Create researchers for projects. Create raters for rating.	High	2
5	Admin	Access all the projects, forum posts, user info	I can have all access to manage everything.	High	2
6	Admin/Researcher	See the allocated raters from the projects created by me (Implied by requirements)	I know who has been assigned to a specific project	Medium	2
7	Researcher	Add/remove raters	I can allocate raters in their allocated projects	High	1
8	Rater	See which projects allocated to me (Implied by requirements)	I know what projects I can have access to and which activities I can complete	Medium	3

Epic 2 - Project and Module Management

No.	As a <Role>	I want to <Do something>	So that <achieve some goals>	Priority	Task Size
1	Researcher	Create a new project and manage it	Different raters will have different access to the projects	High	2
2	Researcher	Make project available at a specific time	Raters can have access during a specific period of time	High	1
3	Researcher	Embed downloadable Word, PDF documents, audio, video, simple surveys and sample texts when creating activities	The activities will be more interactive for raters.	Medium	5
4	Researcher	See a overall summary of frequency of rating levels for each sample	I can know how each sample is rated	Medium	2
5	Researcher/Admin	Download the data (rater's input) from the modules	I can analyse the downloaded data	High	1
6	Rater	Enter a rating below a sample text	I can accurately assess the sample	High	1
7	Rater	Return to my ratings and make changes as needed	ensuring flexibility in my assessments	High	2
8	Rater	Download all the text with highlights included	I can compare two descriptions and highlight their differences	High	1
9	Rater	Reorder chunks of text on the page	I can organise the information in a way that suits my needs	Medium	3
10	Rater	View rating statistics	I can gain overall assessment trends	Medium	2

Epic 3 - Forum Management

No.	As a <Role>	I want to <Do something>	So that <achieve some goals>	Priority	Task Size
-----	----------------	-----------------------------	---------------------------------	----------	-----------

1	Admin/Researcher	Create threads for particular topic discussion.	Raters will be allowed to post their discussion on that threads to share their thoughts.	Medium	3
2	Rater/researcher	Post my ideas/answer on a thread with specific topic.	I can share my ideas to others and look for others' answer as well.	Medium	2
3	Researcher/rater	Reply others' posts.	Join in a discussion to share my answer or ask question further.	Medium	3
4	Researcher/admin	Manage existing posts (Delete, mark)	Duplicated post can be removed, and important post can be highlighted.	Low	2
5	Researcher	Select some activities then transfer their answers to the thread automatically.	Others will be able to reply to those automatic posts.	Low	3
6	Rater	Request admin/researcher to anonymized my response to a particular post.	Keep my privacy.	Very low	4

Non-Functional Requirements

Testing:

- **Unit Testing:** We utilise frameworks to conduct unit tests ensuring individual components and functions operate as intended. Test cases are written in JavaScript to cover a wide range of expected outcomes.
- **API Testing:**
 - **Postman:** This tool is used for API testing to ensure that all endpoints meet their contract in terms of response format, error handling, and performance under load. Postman collections can be shared within the team to ensure consistency and comprehensiveness of API testing.
- **Integration Testing:** To validate the interactions between modules, tools like Mocha or PyTest will be used depending on the programming language in sprint 3.
- **End-to-End Testing:** Tools like Selenium or Cypress will provide automated browser testing to simulate real user scenarios in sprint 3.

Security:

- **Authentication:** Utilises JWTs for secure authentication and session management.
- **Authorisation:** Implements role-based access control (RBAC) to ensure users can only access functionalities relevant to their permissions.

Development Environments:

- **Development:** A local environment where developers can work independently on features without affecting the live product.
- **Pre-production (Staging):** Mirrors the production environment for testing. Changes are deployed here before production to catch any last-minute issues.
- **Production:** The live environment accessible to end-users.

IDE and Tools:

- **Integrated Development Environment (IDE):** Developers can use their preferred IDEs such as Visual Studio Code, IntelliJ IDEA, or others suitable for the stack used.
- **Version Control:** Git, with GitHub or GitLab to manage code versions and collaborate.
- **Continuous Integration/Continuous Deployment (CI/CD):** Tools like Jenkins, CircleCI, or GitHub Actions automate the deployment of code changes to various environments.

Package Managers:

Our project uses **npm** as evidenced by the presence of `package.json` and `package-lock.json` files in our directory. npm helps manage packages required for the project, ensuring that all dependencies are kept up to date and consistent across all environments thanks to the `package-lock.json` file. npm also facilitates the use of scripts that can automate various tasks such as builds, tests, and deployments.

Sprint

[Sprint 1](#)

[Sprint 2](#)

[Sprint 3](#)

Plan For Sprint 2 and Sprint 3

As we already have a better overall understanding of the current project through the communication with our client and with the initial requirements elicitation completed, we are one step closer to start developing the system in the next 2 sprints. This documentation will mainly discuss what should be done in each sprint and how we will develop the system.

Requirements to Develop

During Sprint 2, our team will develop the user management and project/module management functionalities outlined in the provided epics. Here's the plan for Sprint 2:

User Management (Epic 1 From User story 1 to 8):

- Implement user (Admin/Researcher/Rater) login and password management functionalities to ensure secure access and account protection.
- Allow users (Admin/Researcher/Rater) to edit their profiles, including changing names and other details.
- Develop features for adding/removing users, managing permissions, and access control.

Project/Module Management (Epic 2 From User story 1 to 11):

- Enable researchers to create and manage projects, including scheduling, embedding capabilities, and statistical features.
- Facilitate effective data rating for raters, allowing them to enter and edit ratings, highlight/reorder text, and rating offline.

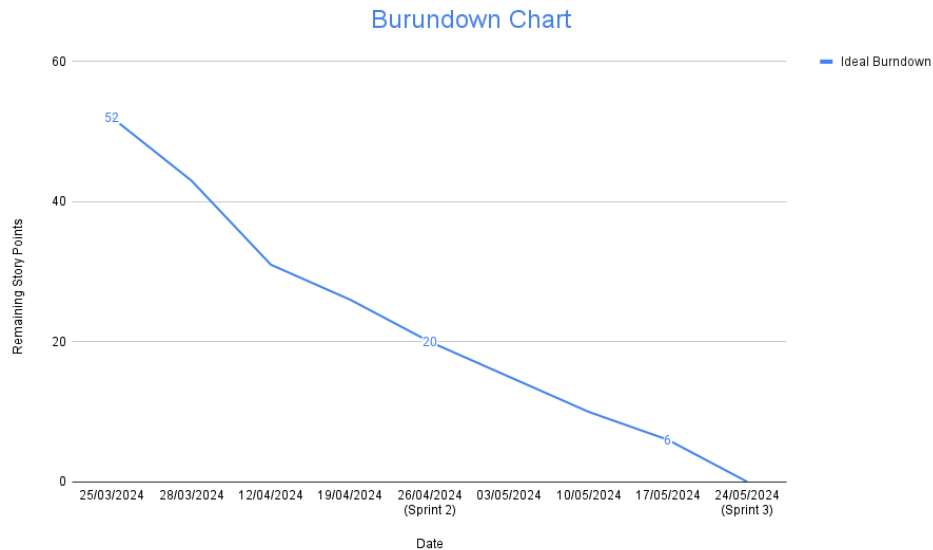
During Sprint 3, we will focus on enhancing the forum management functionalities as outlined in Epic 3. Here's the plan for Sprint 3:

Forum Management (Epic 3 From User story 1 to 6) :

- Admins/researchers can create discussion threads and manage and maintain existing posts.
- Researchers/raters can post their ideas and answers, and reply to others' posts.
- Researchers can transfer their answers to the thread automatically.
- Raters can request the anonymisation of their responses.

Our team has estimated the task sizes and prioritised tasks based on their importance and complexity, ensuring timely delivery and coordination among different functionalities (For more details, see [User Stories](#)). Additionally, appropriate testing and bug fixing will be carried out to ensure product quality and stability.

Below is the burndown chart that we came up with, which indicates the project's velocity and ideal burndown.



Tools and Technologies

After a discussion within our team, we decided to use React.js as our front-end development framework, Express.js as our back-end framework and MongoDB as our database as it works well with Express.js.

React.js is a popular front-end framework that allows us to create reusable UI components for different parts of the website and it also makes it simpler for us to manage the state of the components.

Express.js is a back-end framework for Node.js that simplifies routing, middleware usage and handling HTTP requests. Using Express.js also allows us to use the same language (Javascript) both in front-end and back-end and it will make the development process a lot easier.

In terms of collaboration, we will use Git to manage the version of our codebase and GitHub to host our remote repository. Some features from Git enable better and smoother collaboration. Committing allows us to make changes to our local copy of the codebase and then commit and upload these changes to the remote repository so that other team members can also see the changes. Branching allows us to work on our own branch. For example, if 2 independent features need to be developed simultaneously, we can have 2 different branches for different features so that we can improve the efficiency of the development.

Sprint 1 Review

What we did well in sprint 1:

Collaboration and Teamwork: Our team has excelled at working together, especially when tackling complex problems. There's a strong sense of mutual support, which has led to creative solutions and a positive working environment.

Adherence to Agile Principles: Our team has been consistently good at maintaining the flexibility required by Agile methodologies, effectively responding to changes in requirements and priorities without significant disruptions.

Quality of Work: The delivered work generally exceeds the expected quality standards, with few issues reported after the release of grade. This is a testament to the team's attention to detail and commitment to excellence.

Effective Communication: The team has established a strong communication framework that ensures everyone is on the same page. Regular stand-ups, clear channels on WeChat, and open hours with our client have fostered an environment where information flows freely and efficiently.

Responsive to Feedback: Our team has shown a remarkable ability to respond to feedback, whether it comes from within the team or from stakeholders. This responsiveness is about genuinely considering the feedback, discussing its implications, and implementing it in a way that improves the project while staying aligned with overall objectives.

What we can improve in sprint 2:

Refine Technical Skill Assessment: Given the team's current learning curve with new techniques, it's crucial to assess each team member's technical skills more accurately. This assessment will help in better matching tasks to individual capabilities. By doing so, we can ensure a more balanced distribution of workload and potentially prevent the need to push uncompleted stories to Sprint 3. Additionally, scheduling targeted technical meetings might accelerate the team's proficiency and confidence with unfamiliar technologies.

Emphasise Documentation: Allocating specific times for updating documentation during the sprint, perhaps treating it as a sprint deliverable, could improve this area. Encouraging a culture that values documentation through incentives or recognition might also help.

Sprint 2

Plan For Sprint 3

During Sprint 3, we will focus on enhancing the forum management functionalities as outlined in Epic 3 and implementation of activity functionality listed in Epic 2. Here's the detailed plan for Sprint 3:

Activity Implementation (Epic 2 From User Story 13 to 17):

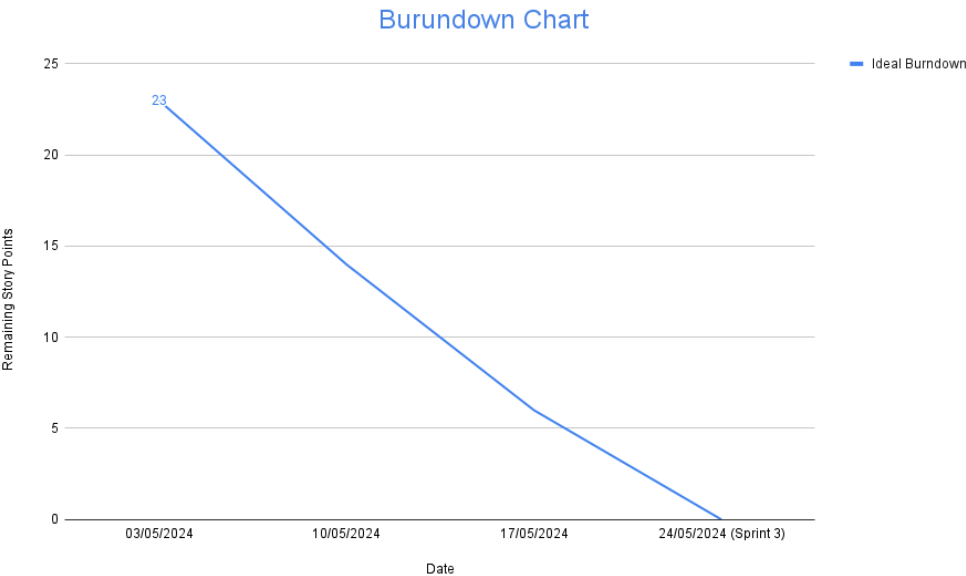
- Researchers can download data from the activities.
- Raters can enter a rating below a sample text.
- Raters can return to their ratings and make changes.
- Raters can highlight text on page and download the highlighted text.

Forum Management (Epic 3 From User story 20 to 25) :

- Admins/researchers can create discussion threads and manage and maintain existing posts.
- Researchers/raters can post their ideas and answers, and reply to others' posts.
- Researchers can transfer their answers to the thread automatically.
- Raters can request the anonymisation of their responses.

Our team has estimated the task sizes and prioritised tasks based on their importance and complexity in sprint 2 (For more details, see [User Stories](#)). Additionally, appropriate testing and bug fixing will be carried out to ensure product quality and stability.

In sprint 3, we will create a new burndown chart. Below is the burndown chart that we came up with, which indicates the project's velocity and ideal burndown.



Sprint 3

Ethics and Security

Cyber Security

Ethical Considerations

Cyber Security

User Authentication

Sign-in JWT (JWT) encryption

- **Secret key:** In order to authenticate users when logging in, a JWT token is generated with the user's ID and a random secret key stored in the server and then is sent to the user. When a user sends a JWT token along with some requests, the server compares this token with one generated from the secret key. If both the tokens are the same, then the user is indeed whom he/she claims to be. The design of using a secret key stored in the server prevents malicious users from forging a fake token with a user ID to log in to someone else's account.
- **JWT lifetime:** Each of the JWT would have a lifetime that specify when the token will be expired. In case where attackers obtain a correct JWT, this design limits the time the attackers can abuse with this token, and potentially reduces the impact from the attackers. This lifetime is subject to change in configuration.

Password encryption, constraints and protection

- **Salt and pepper:** In order to keep passwords safe, when generating a new password, a random salt will be generated in some number of rounds and also be hashed along the password. This design could prevent leaking sensitive information if database is compromised and hashing with salt will make it harder for attackers to decrypt passwords.
- **Password constraints:** When a user is created with a password, it is required that the password would have a minimum length of eight characters. This design is to reduce the chances that passwords are compromised by rainbow attacks because increasing the length of the password would increase the size of the rainbow table.
- **Password storing:** User passwords are not stored in plain text in the database, instead, the passwords are hashed into strings and then these hashes are stored in the database. In case the database is compromised, attackers could not make use of the hashed passwords directly but would also need to obtain the passwords' salts and peppers.

User Authorisation

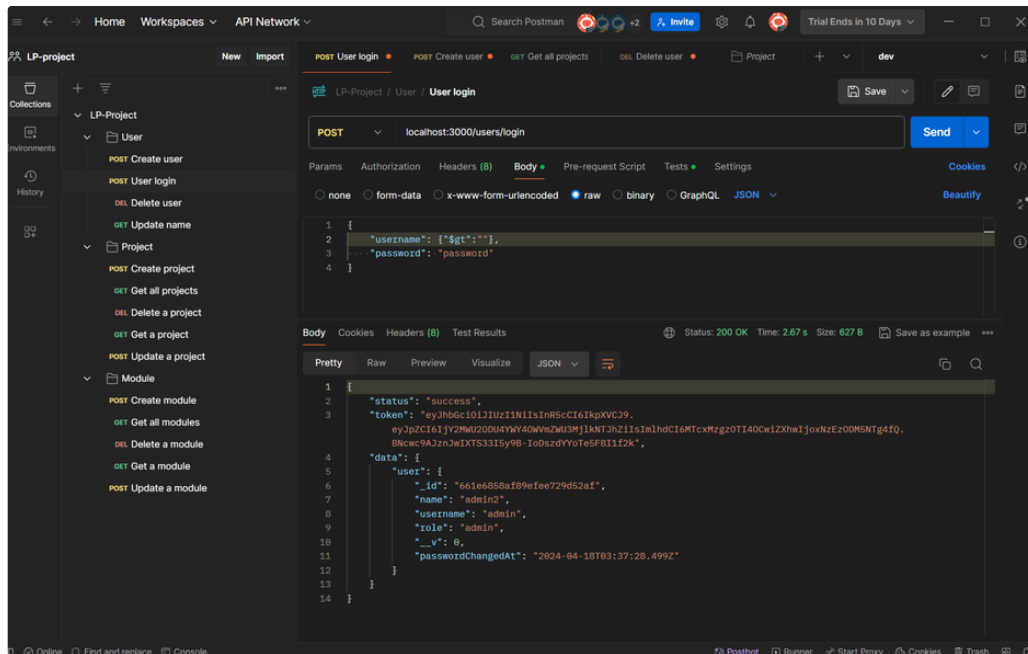
Prevention of broken access control

- **Prevention of Insecure Direct Object Reference (IDOR):** IDOR occurs when an unauthorised user is able to access an object by inputting the object's identifier. In our case, raters can access some other projects or modules which they do not have access to, or researchers can access other researchers' projects without their permission. To prevent IDOR happening, our backend system verifies a user's document access everytime the user requests a document along with the document ID. In the meantime, the system would also run a validator to ensure that the incoming document ID is a valid ID.
- **Least privilege access:** This is a principle in which users are only given minimal access to perform their operations. In our case, some of the functionalities that only researchers and admin can perform – such as creating a project – are never provided to raters at any cases. Raters are only able to obtain information that is relevant to their operations.

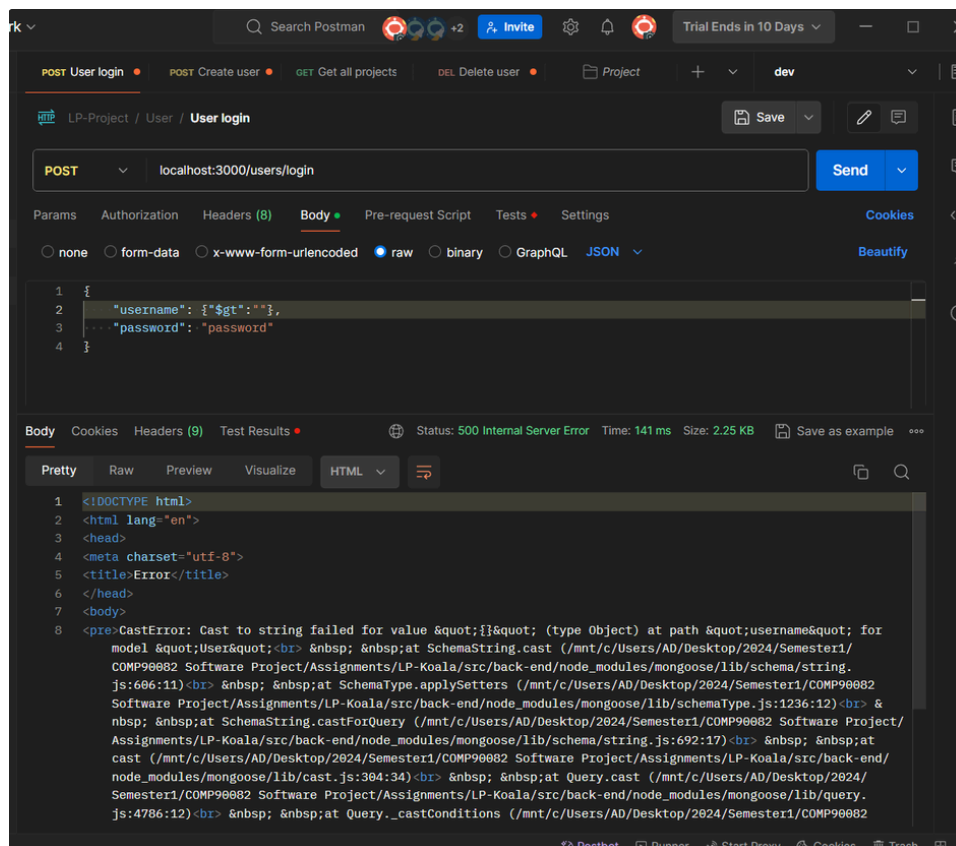
Data validation and sanitisation

- **Data validator:** Validating data is essential to avoid data tampering. In this project, when users are passing a ID to access a particular object, this ID is then validated against the existing object in the database, to ensure that the ID is in the correct format and is valid. For instance, when a rater is passing a project ID to access to a particular project, the system would validate if that ID is valid and really belongs an existing project.

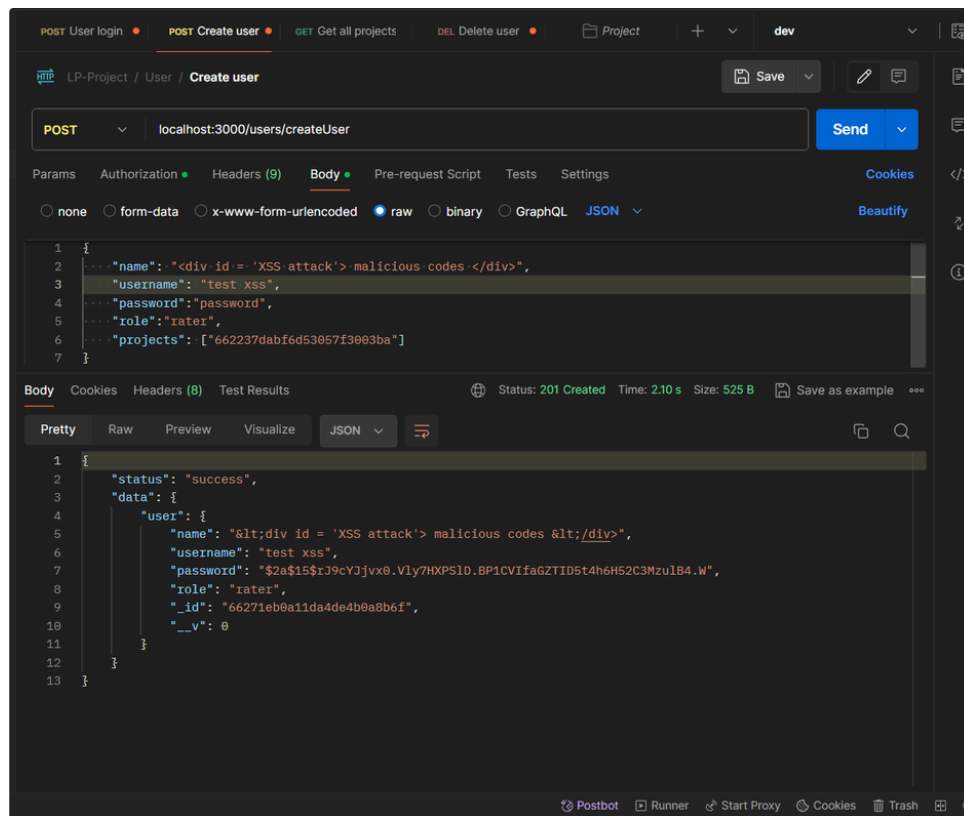
- **NoSQL injection attack prevention:** The system implemented packages to prevent NoSQL injection. An example of NoSQL injection is shown below. This example demonstrates that using NoSQL injection, attackers can bypass the input of username and therefore potentially access admin account.



As a result, packages are used to prevent this from happening. Once protection is implemented, NoSQL injections should trigger errors and will not give attackers access.



- **Cross-Site Scripting (XSS) attack prevention:** Simliar to NoSQL injection protection, XSS protection is also implemented to prevent attackers inserting malicious contents to display misguiding contents to other users (for example, server-side cross-site scripting). The example below shows that sensitive symbols and tags such as `<div>` are converted to other formats to avoid XSS.



- **HTTP Parameter Pollution (HPP) attack prevention:** Similiar to NoSQL injection and XSS attacks, HPP attacks are also prevented with the use of relevant packages. This is to ensure that attackers cannot tamper with parameters, for example, by passing the parameter “username” twice in a request, to cause unexpected damgages to database or to cause data leakages in any way.

Design Concerning About DDoS Attacks and Authentification

- When designing how should an admin create a rater, our team’s initial proposal is first to create a register webpage for raters to input their own name, username and password, and then wait for admin approving for creating their accounts. The admin waould be able to approve or reject the rater’s request in a request inbox. Later, this design raised the concerns in which attackers may send enormous amounts of account creation request as a Denial of Sservice attack. There was also no way to authenticate as to whether the user creating the account is really the person the attacker claims to be. For instance, an attacker may pretend to be a rater Bob and register under the attacker’s email address and password but with Bob’s real name. As a result, our team proposed to stick to the original design in which an admin is able to create a user with role, name, username and password, and then manually distribute account information via email to the corresponding person. Considering the small size of users for this system, this method is applicable and secure.

Logging and Error Handling

- In many of the cases where user performance results in errors, for example, accessing an object without logging in, the system would return an error message to the client indicating exactly that log-in is required. The system will not return an error message that contains the detailed error loggings. As our team is currently in development stage, some of the funcitonalties will still have error loggings, later this project is separated into production and development modes. And in production mode, only necessary error messages are displayed and error loggings will not be returned.

Risk Analysis

ID	Risk Statement	Risk Triggers	Probability (0%-100%)	Impact (1-10)	Risk Justification
1	Failure to uphold authentication in access objects resulting in unauthorised users obtaining credential materials.	Detection of requests to access unauthorised contents.	30% Medium	8 High	<p>Considering that there are multiple objects that can be accessed by three different types of users – admin, researcher, rater – negligence in authentication protection is likely to happen.</p> <p>The impact is high since research materials should be confidential and never be disclosed without permission from their owners.</p>
2	Malicious contents inserted into server due to inadequate data sanitisation against server-side cross-site scripting could result in attackers fishing out users' responses and information.	Detection of uncommon inputs that resembles injection/XSS attacks.	15% Low	7 High	<p>Since the system has employed latest community-well-tested packages to prevent possible NoSQL injections and XSS attacks, it is unlikely that this risk will occur.</p> <p>However, if the attackers find a way to inject malicious HTTP contents via channels such as text responses or comments, users may be misguided to other webpages to give away their user information/responses.</p>
3	Insufficient protection against rainbow attacks or dictionary attacks could result in administrator accounts compromised and important data can be easily obtained with admin's privilege.	Floods of incoming traffic from unexpected sources.	15% Low	10 High	<p>Since the system has employed long, random salt and pepper to hash passwords, and JWT tokens are well protected with reasonable lifetime, it is unlikely that passwords/tokens are compromised by these brute-force attacks.</p> <p>However, if the admin account is compromised, then attackers will gain full access to the data and functionalities of the system, which will lead to disastrous consequences.</p>
4	A critical vulnerability discovered in a third-party package could lead to security of data being compromised,	Failure in third-party security assessments or audits.	10% Low	9 High	<p>Considering that the system has employed popular, well-maintained packages for security and data sanitisation, it</p>

	leading to rater privacy concerns and confidential materials exposed.			is unlikely for the packages to have critical errors. The impact is high since vulnerability in third-party packages could potentially give attackers opportunities to perform injection or XSS attacks, which could result in admin account's compromisation.
--	---	--	--	---

Contingency Plan

Prevent

1. Factory method or middlewares should be used to handle access control as a whole so that extention and maintainance can be made easily, and neglience in this area can be easily identified.
2. Tests should be done in occasion where it requires user's inputs, e.g. comment, username etc.. And so areas to protect can be identified.
3. Employ more methods to protect passwords, which include setting up a limit of incorrect passwod input, using a more secure hashing method such as SHA-512, requesting F2A from time to time when logging in.
4. Keep a list of the third-party packages used, conduct regular audits into third-party softwares' security. Keep track of lasttest critical vulnerability from official sources such as <https://owasp.org/>.

Detect

1. Keep a log of user requests, including as much information as possible, such as time, userID, IP address etc. for further detection or analysis of anomalies. This should be able to detect possible attacks from the risks above.
2. Set a trigger if there is a flood of incoming request so that anomalies can be checked.

Response

1. If attacks are detected and taking affect, it is the best to put down the service and fix the corresponding vulnerability.
2. IP addresses that send out suspicious request should be put into blacklist.
3. Considering the scale of this project, forming a dedicated incidence team will be impracticable. However, communication channels can be established beforehand. Once an incident happens, notifying the affected users would mitigate possible negative effects as user may have time to change password and protect their data.

Recover

1. Assess the extent of damage, including data leakage, server downtime, and possible financial loss.
2. Ensure that the fixed system is thouroughly checked for malwares and other vulnerabilities.
3. Keep users updated with the recovery progress, including researchers and raters.

Ethical Considerations

1. **Data Privacy and Security:** Due to the project involving confidential testing data and maybe some potentially sensitive information, it's pivotal to ensure all the data processing complies with related data protection laws. This includes secure storage and controlled access. Through using encrypted storage solutions such as cloud services providing encryption, we can protect data securely. Meanwhile, by implementing role-based access control, we can ensure only authorised users have access to the specific data. This approach can not only allow relevant team members to have access to the specific datasets, but also minimise the risk of data breaches.
2. **Consent and Transparency:** It's essential to gain the informed consent from testing users and final users, which means providing clear information regarding the purpose of research, what participation involves, and any possible risks. Moreover, don't forget to keep records of consent forms as proof that consent was gained, crucial for compliance with ethical standards and legal regulations.
3. **Anonymity:** As mentioned in the project document concerning the chance of anonymising rater responses, ensuring the anonymity of users' data can greatly help protect their privacy and personal information. In addition, it's ideal to ensure that the data shared with third parties for research purposes is properly anonymised to prevent re-identification of users.
4. **Accountability and Honesty:** Maintaining high standards of honesty and integrity in conducting and reporting research is critical, which included acknowledging all contributors and disclosing any conflicts of interest. The conflicts of interest refer to financial interests, affiliations, or any other factors which may affect the impartiality of the research.

Meetings

Client Meetings

Mentor Meetings

Team Meetings

Client Meetings

14/03/2024 Client Meeting

Date : 14/03/2024

Time: 2:00PM- 2:50PM

Participants: Sally O'Hagan (Client) , Haofeng Chen, Yujin Du, Gaoyuan Ou, Mingxin Li, Weiyang Wu, Qinglin Zhao

Meeting Topic: Discuss and clarify requirements, Walk through motivational models, personas, user stories and low prototypes.

Time	Item	Presenter	Notes
2:05-2:06	Introduction	Weiyang Wu	<ul style="list-style-type: none">• Introduction to the meeting agenda. Request for recording.
2:06 - 2:10	Motivational models and persona	Haofeng Chen	<ul style="list-style-type: none">• Walks through the motivational models and persona
2:10 - 2:16	Persona	Yujin Du	<ul style="list-style-type: none">• Walks through to the persona• Clarification on scalability: increase in functionalities and capacities of the functions as the number of users goes up e.g. the product is still responsive if the number of users increases from 10 to 100.
2:16 - 2:22	Epic 1 Clarification	Weiyang Wu	<ul style="list-style-type: none">• Walks through Epic 1 user management• Clarify on admin's "all access"
2:22 - 2:25	Epic 2 Clarification	Gaoyuan Ou	<ul style="list-style-type: none">• Walks through Epic 2 Researcher requirement
2:25 - 2:26	Epic 2 Clarification	Mingxin Li	<ul style="list-style-type: none">• Walks through Epic 2 Rater requirement
2:26 - 2:31	Clarifications	Sally	<ul style="list-style-type: none">• Clarification on re-ordering chunk of texts: more like re-ordering some pieces of cards that contain texts.• Clarification on rater requirements: must have some ways for the raters to interact with the activity. (re-ordering, highlighting, downloading...)• Clarification on "all access": There will be more clarification to what it means that "admin has all access", how could admins differentiate from researchers? Does an admin also have researchers' functionalities?
2:31 - 2:35	Epic 3 Clarification	Qinglin Zhao	<ul style="list-style-type: none">• Walks through Epic 3 forum

2:35 - 2:44	Clarifications	Sally	<ul style="list-style-type: none"> • Clarification of anonymity : raters have to request for anonymity from admin and researcher. No raters can switch to anonymous by themselves. • Clarification on forum: forum for both standardization and familiarization. • Clarification on standardization and familiarization (starting from 31:20): give raters some sample tests first, raters complete the tests, discuss on the forum. When in standardization, raters won't have that kind of conversation but will provide reasons for their ratings. • Discussion on client feedback • Discussion on priority to see if there is discrepancy
2:44 - 2:49	Low prototype	Weiyang Wu	<ul style="list-style-type: none"> • Weiyang introduces a low prototype. • Suggestion on prototype: maybe to have a forum under each activity instead of under each module. • Clarification on data: sample data to be given to understand what an activity would look like.
2:49-2:51	Question and Answer	All members	<ul style="list-style-type: none"> • Clarification on data security: mainly concern about raters having unauthorized access to other confidential documents. Raters may be asked to read and sign a letter of agreement in regards to confidentiality before doing tests.

Action items:

- Shift of priority of the user stories: focus more on the epic 2 features. (Especially downloading-data feature, important, must-have)
- Edit rater anonymous functionality: raters have to request for anonymity.

Links:

- Due to the limited access of the AI tool, around 5 minutes of audio was cut off. No video provided by the AI tool as well.
- Further meetings will not have this issue again and will be recorded locally via zoom recording.
- [Audio link via Google drive \(access via unimelb email address\)](#)
- [Audio link via Otter](#)

07/03/2024 Client Meeting

Date: 07/03/2024

Time: 11:00AM-11:26AM

Location: ZOOM

Participants: Clients, Mentor, our team, and the other team

Meeting Topic: First Client Meeting of LP

Topic	Content
1. See the clients	<ul style="list-style-type: none">• Provide a brief introduction to the project.• Browse the project information document.• Know the requirements of this project.
2. Q&A	

[Video recording link](#)

Mentor Meetings

06/03/2024 Mentor Meeting

Date: 06/03/2024

Time: 2:00PM-2:32PM

Location: Zoom

Participants: Mentor, our group, the other group

Meeting Topic: Mentor meeting and introduction

Topic	Content
Meeting requirements	<ul style="list-style-type: none">• Write a Minute of Meeting for each mentor, client, stand-up meeting. (Can be done in a rolling-basis)• Attend client meetings to understand their requirements, refine the requirements in the meeting• Mentor only attends the client meeting on this Thursday, then will not attend anymore client meetings
Emailing	<ul style="list-style-type: none">• Assign one person specifically to communicate with the client and the mentor via email. When sending emails to the client, CC to the mentor• Email template: https://cis-projects.github.io/project_based_course_notes/extras/templates_for_comm.html• Do not send emails after working hours• After client meetings, we can send a minute of meeting to the mentor(optional?)
Tasks	<ul style="list-style-type: none">• Decide on task tracking tool, and invite the mentor as well• Complete mentor weekly meeting link:https://www.when2meet.com/?24011586-qEjkc
Introduction/Ice breaker	N/A
Others	<ul style="list-style-type: none">• Make documents clean, presentable, understandable, because mentors from other groups will know our progress and mark our project through these documents

12/03/2024 Mentor Meeting

Date: 12/03/2024

Time: 1:30pm-2:00pm

Location: Zoom

Participants: Haofeng Chen, Lin Li, Weiyang Wu, Gaoyuan Ou, MingxinLi, Yujing Du, Qinglin Zhao

Meeting Topic: Weekly meeting with mentor

Topic	Content
1. Stand up	<ul style="list-style-type: none">• Haofeng Chen and Yujin Du had a discussion and completed the project overview, background, and goals.• Weiyang Wu arranged the meeting with the client for this Thursday 2.pm and continued working on the user stories for Epic 1.• Qinglin Zhao completed the user stories for Epic 3.• Mingxin Li and Gaoyuan Ou had a discussion and continued working on the user stories for Epic 2.
2. Mentor suggestion on Project	<ul style="list-style-type: none">• Discuss Confluence structure: Each sprint can be divided into Planning, Review, Retrospective. Development Environment, Quality, Meetings.• Meeting minutes should be uploaded on Confluence.• Proper project structure should be created on Github.• Keeping using and updating the Trello board.• Can make an acceptance document to get consent from the client about the requirement on Trello.

19/03/2024 Mentor Meeting

Date: 19/03/2024

Time: 1:30pm-2:00pm

Location: Zoom

Participants: Haofeng Chen, Lin Li, Weiyang Wu, Gaoyuan Ou, MingxinLi, Yujing Du, Qinglin Zhao

Meeting Topic: Weekly meeting with mentor

Topic	Content
1. Stand up	<ul style="list-style-type: none">• The team introduces its progress
2. Mentor suggestions on project	<ul style="list-style-type: none">• Can use vertical templates on the Personas• Personas and background can have vertical layout by making them separate pages• Confluence structure: not following the sprint 1,2,3... But instead follow the SDLC structure.• To-Be-Feel: can improve structure, share an example• Task size use user story point, explain what the story point represent• Planning: need a timeline• Github: Project overview, project goal, team introduction, change log, workflow, e.g. many branches, how to merge, what does the merge mean? Branching and merge, pull, review strategies, remember to update• Trello: write a column to explain the trello tasks. Suggestion: only ToDo, Doing, Done, extra info in the card. Can add story points into descriptions.• Introduce the technical skills, Suggestion: can write a summary in the plan, and then write details in a separate section. Analyze the technologies used. Discuss pros and cons

23/04/2024 Mentor meeting

Date: 23/04/2024

Time: 13 : 30 - 14 : 00

Location: Zoom

Participants: Haofeng, Weiyang, Yujin, Qinglin, Gaoyuan, Mingxin

Meeting Topic:

Topic	Decision Making	Actions
Code review	Post issue on ed with explanation. If the problem still cannot be resolved, use chatgpt directly.	
Deployment	Free deployment platform is sufficient. If recording video, user stories should be mentioned.	
Development progress	Still need to accelerate.	
Ethic	Follow the content of the lecture.	
Confluence	Structure improvement	Add more meaningful folders such as plans, meetings. The order should follow software development life cycle.

Team Meetings

13/03/2024 Team Meeting

Date: 13/03/2024

Participants: Weiyang Wu, Haofeng Chen, Gaoyuan Ou, Mingxin Li, Qing Lin, Yujin Du

Meeting Topic: Discuss the user stories that we have made so far; Discuss the target user personas

Time	Presenter	Notes
19:00	Weiyang and other 3 teammates	About the user stories
19:30	Haofeng Chen and Yujin Du	Discuss about the target user personas

Action items:

- Figure out the current problems and discuss them together.
- Demonstrate the current work to the clients.

Decisions:

- Confirm the decisions we made with stakeholders tomorrow.
- Refine the user stories.
- Introduce the personas to clients at the next meeting with clients.

11/03/2024 Team Meeting

Date: 11/03/2024

Time: 14:00 - 15:00

Location: Old Engineering Building Meeting Room G79

Participants: Gaoyuan Ou, Mingxin Li, Qinglin Zhao, Weiyang Wu, Yujin Du

Meeting Topic: Requirement analysis and user stories

Topic	Content
1. Questions from the requirements	1. Discussed some questions or confusions raised from the requirement document from the client. 2. Some still remained unresolved and should be mentioned in the next client meeting.
2. Allocate epics for user stories	1. Discussed on how to convert requirements into epics. 2. Assign people into epics for user stories.
3. Decided time for next meeting	1. Finalised the time for the next meeting, which is 7pm 13/03/2024.

09/03/2024 Team Meeting

Time: 2p.m.

Location: Online

Participants: Haofeng Chen, Weiyang Wu, Mingxin Li, Guoyuan Ou, Qinglin Zhao

Meeting Topic: Sprint 1 plan

Topic	Decision Making	Actions
People for Analysis of requirements	Qinglin Zhao Weiyang Wu Gaoyuan Ou Mingxin Li	Prepare user story
People for Background description	HaoFeng Chen YuJin Du	Prepare project overview, background and goals
People for Confluence	WeiYang Wu	Organize Confluence
Meeting for analysis of requirement	Hold on 11/3/2024 2p.m. 3 in person with Zoom	Hopefully finish requirement analysis and start to plan next sprints

21/04/2024 Team Meeting

Date: 21/04/2024

Time: 21:00 - 22:00

Location: Zoom

Participants: Gaoyuan Ou, Mingxin Li, Qinglin Zhao, Weiyang Wu, Yujin Du, Haofeng Chen

Meeting Topic: Sprint 2 Progress

Topic	Content
Stand up	<ul style="list-style-type: none">• Front-end Progress Showcase:<ul style="list-style-type: none">◦ Gaoyuan Ou, Mingxin Li, Haofeng Chen present the progress on the front-end.◦ Mention that the front-end development is almost complete except for a part of the activity.• Back-end Progress Showcase:<ul style="list-style-type: none">◦ Qinglin Zhao, Weiyang Wu, Yujin Du present the progress on the back-end.◦ Note that the back-end development is almost complete except for a part of the activity.
Questions and discussion	<ul style="list-style-type: none">• Address any questions or concerns raised during the progress showcase.• Discuss issues encountered during the showcase and add them to the fixing list.• Hold a discussion on how data is related in the back-end, focusing on the relationship between users and projects.• Discuss the issue with uploading files to MongoDB and brainstorm possible solutions.
Next Steps	<ul style="list-style-type: none">• Start working on the document in Confluence• Keep doing the remaining part of development.

AI Code Review

Sprint 2 Code Review

Sprint 2 Code Review

AI Model: ChatGPT 3.5

People Participated: Qinglin Zhao

Date: 29/4/2024

Code Review Target: Back-end essential logic code and entity model.

Reviewing Method:

This code review work should have been completed through GitHub integration. However, problems occurred during use and were not resolved in time after feedback. Therefore, this code review was completed by manually entering the query content into ChatGPT (using consistent prompt words).

Selection Criteria for Reviewed Code:

It is not a wise choice to review all files. First, you must remove irrelevant content such as configuration files. Additionally, because a lot of the code is just structural parts of the entire application, there isn't much that needs to be tweaked. This type of code files are mainly routing files in the back-end code structure, so route files are not involved in this code review. The main files for this code review are controller files and model files. The controller file mainly handles the request processing logic in the application, while the model file mainly handles the business logic in the application.

Feedback Summary:

According to the prompt words, the feedback provided by AI includes: documentation defects, visual representation defects, structure defects, new functionality, resource defects, check defects, interface defects, and logic defects. I will summarize each item in the following.

1. **Documentation defects:** Naming is generally fine since every developer in the group followed good software convention. About commenting, AI told us to be more detailed and provide context for the logic.
2. **Visual Representation Defects:** Bracket Usage, indentation and long line problems are fairly few.
3. **Structure defects:** This part included detection of dead code and duplicated code. Dead code has not been discovered in our code. However, we do have some duplicated code.
4. **New functionality:** Our code followed the standard of express framework and mongoose model.
5. **Resource Defects:** All variables are properly initialized before use and memory usage seems fine.
6. **Check Defects:** Input check was included in the code, but it could be more robust depending on requirement.
7. **Interface Defects:** Parameters seem appropriately used when calling functions and libraries.
8. **Logic Defects:** The logic appears to be correct, but there might be some edge cases that need more thorough testing and the performance seems acceptable for typical use cases.

Recommended Changes from AI are generally consist of:

- Add comments to explain the purpose and functionality of specific sections of code, especially complex logic or business rules.
- Refactor duplicated code blocks into reusable functions or middleware to improve code maintainability and reduce redundancy.
- Enhance input validation to handle edge cases and ensure data integrity.
- Consider optimizing database queries to improve performance, especially in operations that involve fetching or updating multiple documents.

Respond to AI feedback:

After receiving feedback from AI on our code, we considered the feedback and came to the following conclusions based on the actual situation.

AI has a strong ability to detect code structure and format, and it is also easy to find duplicate codes in the code. When evaluating the UserController.js, the AI discovered that a portion of the logic in our code was used multiple times. Therefore, a refactoring suggestion to

wrap it into a function was proposed.

b. Duplication: There's some duplication in the logic for handling ``req.body.researchers``. This could be refactored into a separate function to avoid repetition.

Duplication found by ChatGPT

However, except the ability of check basic code problem, the suggestions provided by AI only improve the content mentioned in the prompt words, and do not give us more specific details and suggestions. We think the reasons are as follows. The first and most important point is that AI can only process one file at the same time when conducting code evaluation, and cannot associate files to view them together. Our code is structured into Route, Controller and Model. These three components are in a calling relationship, so just looking at the code of one part of them alone cannot get a lot of useful information. This is why the AI will often say that the code seems reliable because it doesn't know what the other parts are like.

In addition, the space for AI to play under this prompt word is limited. AI will only answer one by one based on the entries in the prompt word. For these prompt words, AI can only use some general answers. This is reflected in the fact that no matter which code file I use, the feedback I get is actually similar.

Action Taken:

Based on the above analysis, we believe that the current AI code review obtained under the prompt words cannot provide us with a lot of useful information. However, some basic problems such as duplicate code can still be corrected, so we will also refactor the code in this part. However, the answers given by other AIs are still too general, so there are not many modifications at this stage.